Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.413 – 417

Protect Intranet the Usage of Embedded and Allotted Firewall Machine

S.Boopalan
Assistant Professor, Department of Computer Applications, KG College of Arts and Science, Coimbatore

ABSTRACT: Due to the effect of the rapid popularization of net and e-trade, most businesses and organizations take extraordinary attempt to shield their data systems against malicious assaults and invasions. The firewall is the maximum familiar method among applicable technology for net protection. However, the firewall structures in use today are either utility software or utilities walking on the private computers or network nodes. Its miles very inconvenient to put into effect and manipulate the traditional firewalls. so that you can make the management and production of them less difficult without disrupting the present community topology, we enforce an embedded and disbursed firewall machine to protect the net. On this way, we integrate the features of the firewall and a crucial safety coverage server into an embedded gadget, which may be realized as a community interface card.
Keywords: Distributed and Embedded Firewall, Firewall, and Intranet and Security.

1. INTRODUCTION

The internet and the e-begin are an increasing number of popular in current years. Researchers at the community security technologies have turn out to be very critical for each authorities companies and commercial enterprise companies [1].

To investigate the security technologies in use, Gordon et al. display that use of firewall technologies is the maximum famous amongst their respondents in U.S. [2]. Use of the firewall technology is accounted for ninety seven% of the 687 respondents. However, most firewalls in use are primarily based at the conventional firewall architecture. They consist of either software program or utilities going for walks at the laptop or community nodes. The conventional firewalls are typically set up on the access point of the community for the employer or organization.

Some of serious troubles of the conventional firewalls can manifest. First, for the reason that these firewalls are set up in a single choke point, if the firewall is damaged because of energy outage or flooding assaults, all computer systems in the intranet can be disconnected to the internet. Second, the intranet risk is likewise a trouble confronting management records structures (Management Information Systems) in lots of corporations. As an example, if a worker inadvertently opens a malicious e- mail from the internet and

infects his pc with a Trojan horse. Abruptly, all of the other computer systems inside the identical intranet would be infected with the bug thru this employee's computer.

Therefore, I suggest to implement a distributed security device implemented with an embedded firewall to improve the performance of the traditional firewall. And this allotted protection machine is proven to now not most effective have functions of traditional firewalls however also be able to work in opposition to intranet threats.

2. BACKGROUND

The firewall technology will be classified into 3 classes [3-7]: 1. Packet Filtering 2. Stateful examination 3. Application Proxy. The Packet Filtering is that the earliest methodology employed in the firewall technology. It usually works within the Network Layer of the OSI network module. After it, the Dynamic Packet Filtering continues to figure up to the Transport Layer of the OSI network module. This technology is employed to watch the Network Layer and Transport Layer, and analyze knowledge of every packet, like the header, the protocol, and also the supply address, etc. The firewall can then validate knowledge by rules of the firewall filter. If a packet is judged to be denied, then the firewall can drop it. However, this methodology isn't perpetually helpful against flooding attacks.

The Stateful review firewall uses a module referred to as stateful review to intercept the information it wants in each OSI network modules. and also the advantage of this technology is that the accessing and analyzing method doesn't have an effect on works on any OSI network module, i.e. the firewall is clear to the network users. The Application Proxy technology operates in the Application Layer, i.e. the highest layer of the OSI network module. It can implement higher level of detection technology to defend Internet attacks. For data transfer, it uses a proxy server to transfer data from the source to the destination. This process can let the user feel that no lag existing when connecting to the server.

Fig.1 shows structure of the standard firewall theme normally employed in organizations and firms. The network to choose whether or not to transfer knowledge between computers and therefore the web or not is controlled by the firewall cluster. However, this structure has weakness underneath flooding attacks. If the attack succeeds, the broken firewall can become the bottleneck for the network.

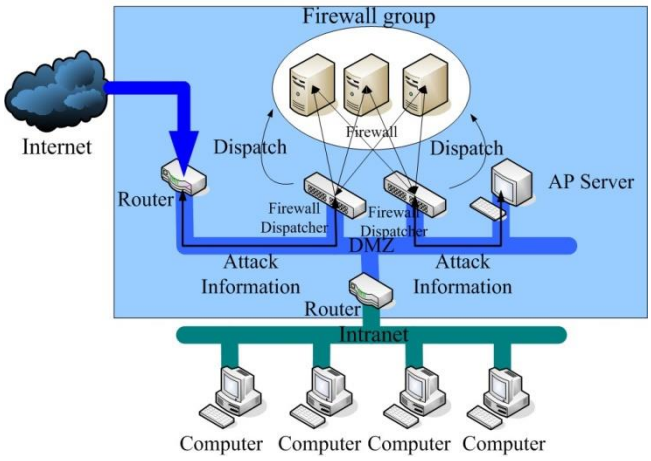

Figure 1. Structure of conventional Firewall Scheme

On the opposite hand, Koch argued that the within attacks causes a lot of monetary price than the surface attacks [8]. as a result of this, the non-public firewall has become a replacement trend to realize network security. Bellovin planned a Distributed firewall thought by victimisation the all host firewall strategy to resolve issues of the standard firewall structure [9-11].

In this paper, my analysis is target transfer of the firewall work layer from Application Layer to the information Link Layer. This idea is to undertake to scale back the influence created by the firewall to original process works within the pc. Therefore, we are going to build a firewall structure in conjunction with associate on-board processor and a memory network interface card. Within the different words, we are going to build a firewall module within the network interface device.

3. STRUCTURE OF DISTRIBUTED SECURITY SYSTEM

The style of a Distributed Security System (DSS) structure to notice intrusions. In Distributed Security System, variety of style goals ought to be taken care of once implementing it. First, the system ought to have a management mechanism, the central security policy server. Second, it should be a general module style. Third, the system ought to have each the functions of standard firewall and the distributed characteristic for preventing attacks of the web and threats of the computer network.

In the DSS structure, the foremost necessary half is implementation of the non-public firewall. We use AN embedded system to implement this half. There is variety of advantages by exploitation the embedded system. The embedded system has its own management processor unit and memory. It additionally has the network and USB interfaces. Therefore, we are able to build the firewall module on the embedded system by connecting the embedded system to the pc by USB interface and connecting the embedded system to the web by Network interface at a similar time. It has a tendency to use the embedded system as a Network Interface Card (NIC).

Fig.2 shows the structure of the Embedded Firewall (EFW). The Central Security Policy Server (CPSP) is employed to validate the firewall rule EFW. EFW is employed as a Network Interface Card (NIC). It responds to the remainder of the network and therefore the shopper laptop. The shopper laptop may be a traditional user within the computer network protected by DSS. And EFW is connected with shopper PCs by USB transfer lines. Due to the USB interface, the embedded firewall mechanism is in a position to realize the generic module style and EFW becomes a conveyable detection device.

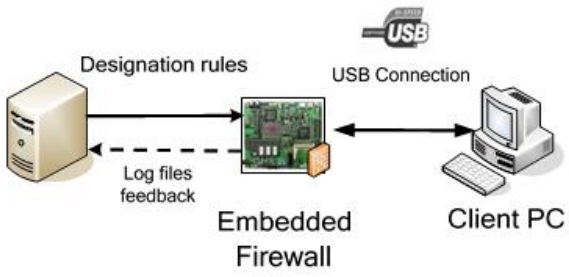

Figure 2. The Structure of Embedded Firewall

DSS consists of 3 mechanisms: 1. Central Security Policy Management 2. Embedded Access management 3.Intrusion Detection Feedback. Fig.3 shows the structure of the DSS with the 3 mechanisms. The Central Security Policy Management mechanism offers

completely different levels of privilege for all the EFW within the system surroundings. The network manager will discovered the extent of privilege with completely different EFW. The mechanism ends up in the goal of achieving level management.

The Embedded Access management mechanism is employed to regulate each EFW. All firewall rules on the EFW are going to be controlled by the CSPM. The CSPM will designate and alter the firewall rule to the EFW. The mechanism allows the EFW to own the packet filter operates. During this mechanism, the EFW also can come back log files to the CSPM, if needed.

The Intrusion Detection Feedback Mechanism collects the log files from Embedded Firewall. And then the mechanism sends the log files to the Intrusion Detection System (IDS) that analyzes the information of the log files and returns the result to CSPS. Consistent with the same results, CSPS adaptively changes the firewall packet filtering rules with every EFW. So, it will dynamically regulate intrusion detection rule for every EFW.

4. RESULTS

DSS with EFW structure on the embedded system with Associate in Nursing Intel XScale processor PXA270, a USB 1.1 interface, and a 10M/100M normal network interface.

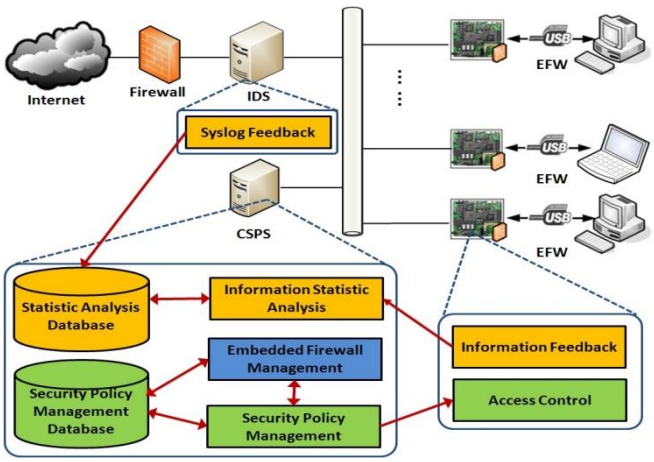

Figure 3. The Structure of the DSS

By putting in the foundations of EFW, we have a tendency to verify that the embedded firewall system made denied ping flooding attacks from the net. Moreover, by setting the access right of the network, EFW was found to be able to management network activities of the computer network users. Additionally tested the planned structure underneath wired and wireless network environments. To downloaded ISO files with the file size over 2GB from a neighborhood FTP website. For the wired setting, the experimental results show that the average transmission rate will attain 950KB/s between consumer laptop and therefore the web that shows the potency of my EFW. If we have a tendency to replace the USB1.1 interface with USB a pair of.0 interface, we'd be able to get far better results.

For the wireless setting, the experimental results show that the common transmission rate can do 550KB/s between shopper computer and therefore the web, that is slower compared to the wired setting. The wireless network card changes the mackintosh address of packets, thus overtime is spent to method packets coming back through the wireless network.

5. CONCLUSIONS

In this paper, I have a tendency to propose a structure to implement the distributed firewall system. I have a tendency to implement the thought of the distributed firewall to effectively forestall attacks and threat from each the web and therefore the computer network. And that conjointly mix the functions of firewall and therefore the central security policy server into the embedded system as a network interface card. The experimental result shows DSS with EFW structure accomplish the goal of implementation of associate degree freelance firewall that is transportable and convenient.

For the long run work, I tend to decide to do stress testing on planned DSS with EFW structure to verify its hardiness below a significant load of traffic. Besides, I tend to decide to do numerous kinds of attacks to validate that my planned structure may be accustomed improve web security for users.

REFERENCES

[1] T. Holz, S. Marechal, and F. Raynal, "New threats and attacks on the World Wide Web," Security & Privacy, IEEE Volume 4, Issue 2, March-April 2006, pp.72 – 75.

[2] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, "CSI/FBI Computer Crime and Security Survey," 2005. Available at http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf.

[3] R. W. Cheswick and S. M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker." Addison- Wesley, 1994.

[4] M. R. Lyu, and L. K. Y. Lau, "firewall Security: policies, testing and performance evaluation," The 24th Annual International Computer Software and Application Conference, COMPSAC 2000, pp.116-121.

[5] R. Zalenski, "Firewall technologies," IEEE Potentials, Vol. 21, Issue 1, 2002, pp.24-29.

[6] Linux Firewall Project: Available at http://www.linuxfirewall.org.

[7] R. Zalenski, M. Boucher, J. Morris, and H. Welte, The netfilter/iptables project, Available at http://netfilter.samba.org.

[8] L. Z. Koch, "outsourcing Security," ZDNet Interactive iWeek, June 22, 2000.

[9] Steven M. Bellovin, "Distributed Firewalls", Journal of Login, November 1999, pp. 39-47.

[10] F. Stevens, T. Courtney, S. Singh, A. Agbaria, J. F. Meyer, W. H. Sanders, and P. Pal, "Model-Based Validation of an Intrusion-Tolerant Information System", from the 23rd Symposium on Reliable Distributed Systems (SRDS'04).

[11] M. Atighetchi, P. Rubel, P. Pal, J. Chong, and L. Sudin, "Networking Aspects in the DPASA Survivability Architecture: An Experience Report", Fourth IEEE International Symposium on Network Computing and Applications (NCA'05)27-29 July 2005, pp.219 – 222.

